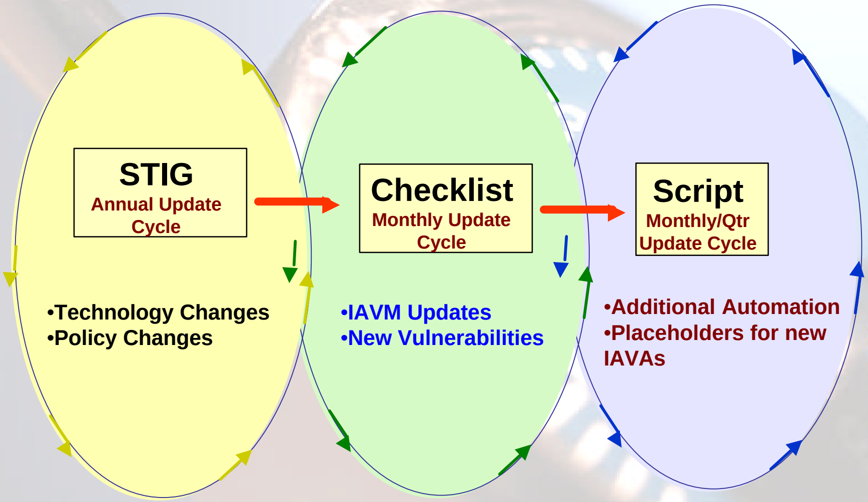
Security Technical Implementation Guides (STIG) and Checklist Overview

Jim Govekar
DISA Field Security Operations
govekarj@ritchie.disa.mil
(717) 267-9275

Agenda

- STIG / Checklist Lifecycle Overview
- What is a STIG
- STIG Lifecycle
- Checklists and Scripts
- Checklist / Scripts Lifecycle
- Available STIGs / Checklists
- Application of STIGs and Checklists

STIG and Checklist Lifecycle



STIG
Annual Update Cycle

- Technology Changes
- Policy Changes

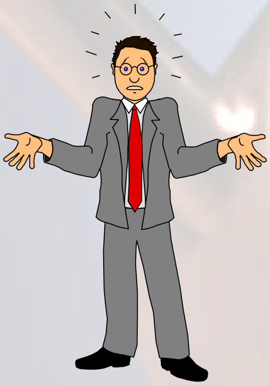
Checklist
Monthly Update Cycle

- IAVM Updates
- New Vulnerabilities

Script
Monthly/Qtr Update Cycle

- Additional Automation
- Placeholders for new IAVAs

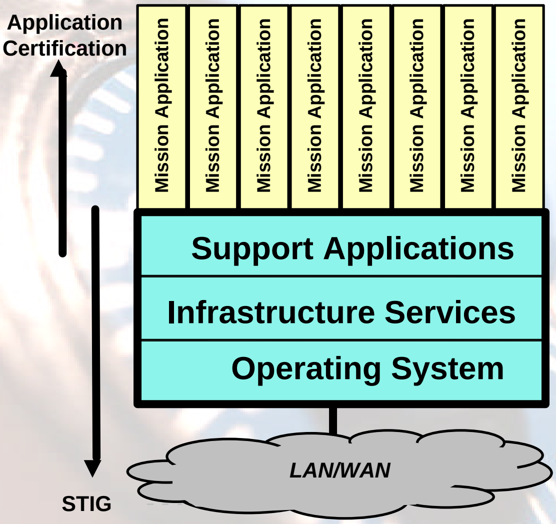
What is a STIG?



- Security Technical Implementation Guide: A Compendium of Security Regulations and Best Practices from Many Sources A Guide for Information Security
- GOALS
  - Intrusion Avoidance
  - Intrusion Detection
  - Response and Recovery
  - Security Implementation Guidance

STIG Scope

- Provides Standard, Secure environment for application development and operation
- Does not replace requirement for application security policy

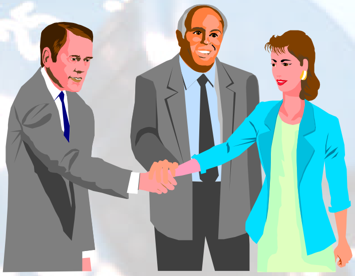


The STIG Lifecycle

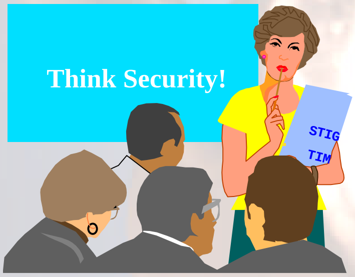
- All STIGs Follow a Standard Lifecycle
  - New STIG Identified
  - Technology Research to Include Existing Guidance if Available
  - Draft STIG is Developed for Internal Review
  - Draft STIG is Distributed to Security Community for Review
  - Technical Interchange Meetings (TIM) with Security Community to Address Issues
  - Changes Made Based on Feedback From TIM
  - STIG is Reviewed by Technical Editing Staff
  - Final STIG is Released to Security Community
  - Checklist and Script Process Begins

Who Writes Them?

- Field Security Operations with input from:
  - DECCs & DECC Detachments
  - SSOs
  - Combatant Commands
  - RNOSCs
  - CERTs
  - Other Agencies, Branches and Organizations
  - Central Design Activities

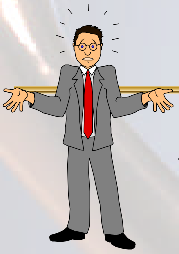


How STIGs are Updated

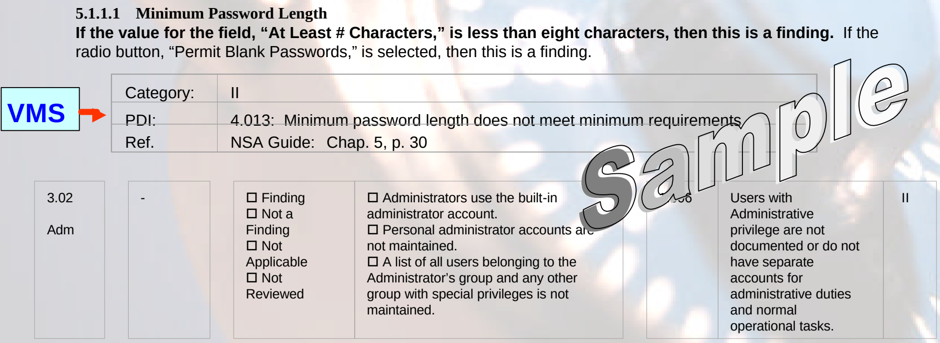


- Internal Technical Guidance
  - Experience In the Field/System
  - Contractor Support
  - Vendor Training
  - IAVM/CERT Notices
- Customer Input
  - E-Mail
  - Technical Interchange Meetings
- Cooperation and Interaction
  - NSA
  - JIEO
  - DOD CERT

Checklists



A Tool that Provides Detailed Instructions for Checking the Presence of a Vulnerability Identified in the STIG Policy



5.1.1.1 Minimum Password Length

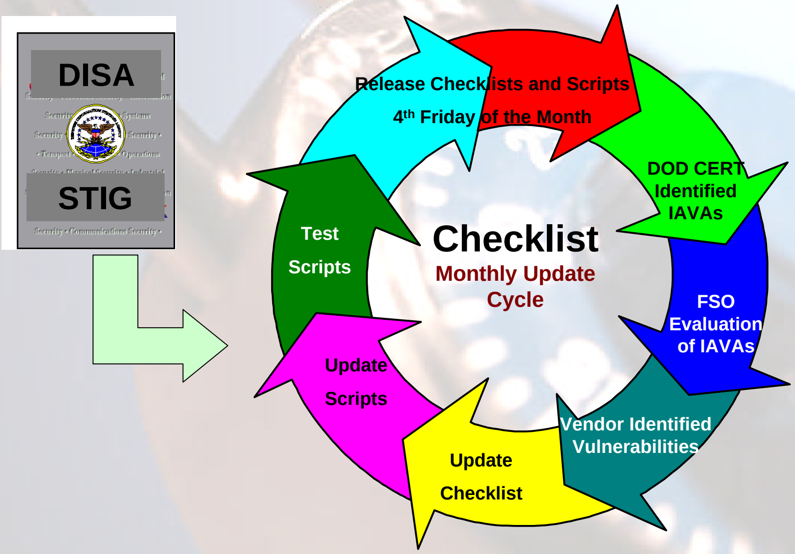
If the value for the field, "At Least # Characters," is less than eight characters, then this is a finding. If the radio button, "Permit Blank Passwords," is selected, then this is a finding.

VMS

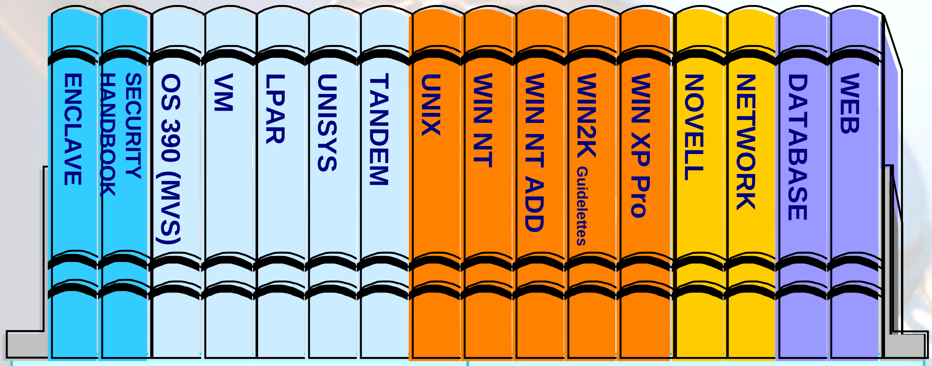
Category:	II
PDI:	4.013: Minimum password length does not meet minimum requirements
Ref.	NSA Guide: Chap. 5, p. 30

3.02 Adm	-	☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	☐ Administrators use the built-in administrator account. ☐ Personal administrator accounts are not maintained. ☐ A list of all users belonging to the Administrator's group and any other group with special privileges is not maintained.	06	Users with Administrative privilege are not documented or do not have separate accounts for administrative duties and normal operational tasks.	II

The Checklist Lifecycle



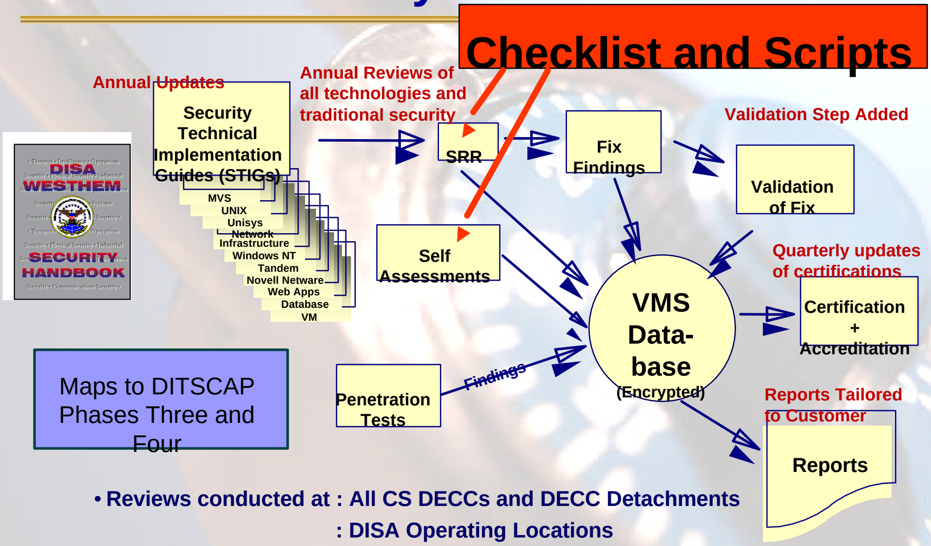
DISA Security Guides



Guides are available at the following Web Sites:
https://iase.disa.mil
http://iase.disa.smil.mil
https://guides.ritchie.disa.mil

- DOD PKI Certificate Required**
- Annual updates
- IAVA Alerts, Bulletins and TA updated monthly to checklist
- stig_comments@ritchie.disa.mil

DISA Information Systems Security Readiness Process



Checklist and Scripts

Annual Updates

Security Technical Implementation Guides (STIGs)

MVS
UNIX
Unisys
Network Infrastructure
Windows NT
Tandem
Novell Netware
Web Apps
Database
VM

DISA WESTHEM SECURITY HANDBOOK

Annual Reviews of all technologies and traditional security

SRR

Self Assessments

Fix Findings

Validation Step Added

Validation of Fix

Quarterly updates of certifications

VMS Data-base (Encrypted)

Certification + Accreditation

Penetration Tests

Findings

Reports Tailored to Customer

Reports

Maps to DITSCAP Phases Three and Four

- Reviews conducted at : All CS DECCs and DECC Detachments
  : DISA Operating Locations
  : Combatant Commands
  : Central Design Activities

Review

- STIG / Checklist Lifecycle Overview
- What is a STIG
- STIG Lifecycle
- What are Checklists and Scripts
- Checklist / Scripts Lifecycle
- Available STIGs / Checklists
- STIG and Checklist Application

Questions?

Thank You for Your Attention!

Jim Govekar
DISA Field Security Operations
govekarj@ritchie.disa.mil
(717) 267-9275

stig_comments@ritchie.disa.mil